
It is very exciting to see so many issues of Cipher in such a short time. Thanks to all of you who have provided material and thanks to Carl for bringing together the issues.

All in all the TC has seen a general increase in level of activity this year.

In November, Carl Landwehr attended the semi-annual IEEE Computer Society Technical Activities Board (TAB) meeting. This is the governing board which oversees all TC activities. This is mostly a business meeting, but there were several topics discussed which are relevant and several topics which resulted in action items for our TC.

The most interesting news is that the CS and the TAB are working towards electronic publishing and providing TC newsletters on line.

The TAB had initially established a goal of having electronic newsletters on the info-server for half the TCs by December 1994. It doesn't appear that they met this goal, but they are continuing to work towards it and CIPHER is among the first newsletters available via the server.

The CS Staff and volunteers are also beginning to experiment with electronic publishing and archiving. In the near term, they are working to make conference proceedings (postscript) available on line to anyone who wants them. Long term, they want to become the central repository for all IEEE CS published documents. They seem willing to try out various approaches, including providing periodic backups of materials (such as Cipher, at present) where more volatile versions are stored elsewhere. We are looking into making abstracts of the Oakland papers available this way in advance of the conference and possibly full texts at a later time. Oakland authors, think postscript!

CS staff contacts for more information on electronic publishing are: Mark Haas (m.haas@computer.org) and Perri Cline (pcline@computer.org).

At the TAB meeting we were reminded that we need to establish a nominating committee and balloting process for electing TC Chairs. In

the past we have used our annual meeting which is held in conjunction with the Oakland conference to elect officers. This year we will need to use a more formal process. In the past we have elected a TC Chair and a Vice Chair. Each serves a two year term, with the Vice Chair automatically moving to the Chair position after two years. This year is an election year as my term will end in June 1995 and Deborah Cooper will move from Vice Chair to Chair, leaving open the Vice Chair position.

I am looking for volunteers to form a nominating committee. In addition to the nomination process, this committee will also need to define a balloting process which meets the TAB guidelines. We have been told that some form of email voting is acceptable. Perhaps we need a subcommittee to define a secure/anonymous e-mail balloting scheme :)

This is a serious matter and one which requires action soon. Please contact me if you would like to volunteer for this committee.

Terry Vickers Benzel
Chair Technical Committee on Security and Privacy

Letter from the Editor

I suppose I am tempting fate by publishing the first issue of the new year on Friday the 13th, but I recently learned from Pierangela Samarati that in Italy, it's 17 that's considered unlucky -- so perhaps delaying this until Tuesday wouldn't help!

Thanks to the many contributors who continue to make Electronic Cipher possible. It's more than a little work to document a conference as thoroughly as Cynthia Irvine has done in her report on the Tenth ACSAC, and I hope you will let her know (irvine@cs.nps.navy.mil) if you find her write-up useful. Thanks also to Avi Rubin for his account of security-related activities at the December IETF meeting.

The Common Criteria were released in December as planned and this issue tells you where to get a copy (though I'm not sure what to make of the label "Draft Version 0.9" -- is this an alpha test version? Or pre-alpha?). The CD-ROM is a great deal easier to carry than the 800

pages of paper would be, but if you don't have PC-compatible handy, you may find it simplest to browse the ascii copies Charles Payne has posted at URL <http://www.itd.nrl.navy.mil/ITD/5540/cc>.

This issue also carries announcements concerning a major, established archive site (COAST at Purdue) and a hopeful new initiative from Canada (FORMIS) that is seeking help from Cipher readers.

The "who's where" column mentioned last time premiers in this issue; it provides a place for people moving to new positions to let their colleagues know where to find them.

For efficiency, the Calls for Papers, Reader's Guide, Interesting Links sections will include only postings new since the last issue; full lists are available in the hypertext Cipher.

Carl Landwehr
Editor, Cipher

Oakland Program Committee Meets; 5 minute abstracts solicited

Members of the Program Committee for the 1995 IEEE Symposium on Security and Privacy assembled shortly after New Year's at the Naval Research Laboratory to select the papers to be presented at this year's Symposium. From 72 submissions, about twenty papers and two panels have been selected for presentation. The advance program will be released in a few weeks, following notification of authors; I believe it will be an excellent meeting. Readers are reminded that for the first time this year an hour has been set aside for 5-minute research reports on current work. If you would like to have a chance to present your latest ideas to the Oakland audience, send a one-page abstract to Cathy Meadows not later than April 3.

The Symposium will be held Monday, May 8, through Wednesday noon, May 10, at the Claremont Resort Hotel, Oakland, California. Meeting rooms can be made available at the hotel Wednesday afternoon, Thursday, and Friday, May 10-12, in conjunction with the Symposium. You may be able to both reduce your total meeting costs and draw a better attendance than if you schedule your meeting separately; please contact the Editor

if you are interested.

Announcement of WWW INFOSEC Site: FORMIS INFOSEC Archive

FORMIS (Framework and Open Reference Model for Information Security) is an informal effort to develop a common reference for information technology security which can provide a way for diverse groups to interrelate their efforts.

In particular, FORMIS is intended to be a repository of information technology security (INFOSEC): terminology, models, support tools, management documentation, training/self-education documentation, product profiles/specifications, bibliographies and on-line papers, and other INFOSEC related items.

The FORMIS Archive and Forums are committed to the following objectives:

1. Identification of those principles, theories, and practices which are fundamental and foundational to the establishment of effective INFOSEC. This basis should form a common and open reference model for information technology security;
2. A procedure for revising the identified basis as necessary to reflect new requirements and knowledge;
3. The dissemination and development of the basis of INFOSEC in a coherent manner which **REDUCES** confusion and **IMPROVES** the general understanding of the basis of INFOSEC at various levels of technological literacy;
4. The establishment of a referential framework which provides for explicitly identifying the relationship between any two things (models, activities, processes, etc.) or between a specific thing and the basis;
5. the identification of a toolset which conforms to the referential framework and functions on the basis; that is, tools which enable individuals and organisations to move toward **THEIR** INFOSEC objectives but which are consistent with the **COMMON** "basis" of "fundamental principles, theories, and practices" and the

"referential framework".

This basic set of tools would be an initial INFOSEC toolkit which would grow and develop as necessary and would support specific activities throughout the INFOSEC lifecycle. Specific tools of near-term interest are those supporting requirements analysis and specification, design analysis and specification, evaluation, acquisition, composition of large systems and risk management.

6. the establishment of an electronic INFOSEC library. This is not just an arbitrary database or repository of documents. The word "library" implies a body of knowledge STRUCTURED and CATALOGUED in some meaningful way.
7. To produce an open task list which is within the terms of the FORMIS charter and objectives and which identifies specific contributions (research, sample policies, models, products, tools, etc) which would contribute to the objectives of FORMIS (stated above).

FORMIS is a contributor driven archive. There is no single ubiquitous source of INFOSEC information and experience. The archive is intended to be a central node to an Internet Web of INFOSEC information. The resources in any one or two (or even three or more) organisations are not likely to be sufficient to generate the kind of framework, model base, and information repository envisioned. The archive will be what those who participate make it.

The short-term plan for FORMIS is to:

1. Survey the World Wide Web, Internet, and the INFOSEC literature for any and all information which might prove helpful in resolving aspects of information technology security which are, as yet unresolved;
2. Provide access to all identified/contributed information resulting from the survey from one site (and from/through collaborating sites, if such are established);
3. Begin the development of a semi-formal model of the information (taxonomically, ontologically, and epistemologically) so that it

does not just become a big electronic slag heap. The longer term objective is a formal model;

4. Begin the development of a dictionary of INFOSEC terminology which is logically structured and which is (relatively easily) parseable by computer applications;
5. Begin the development of a thesaurus of structural and behavioural relationships which exist among the elements of information technology security (these elements must first be identified in the dictionary); and
6. Begin the development of a taxonomically structured model library in which the similarities and differences between and among models are explicitly identified in some formal way.

The home page for FORMIS can accessed through the URL:

<http://www.cse.dnd.ca/~formis/>

FORMIS is hosted on the Communications Security Establishment (CSE) Web server www.cse.dnd.ca and the CSE home page is:

<http://www.cse.dnd.ca/>

It should be noted that although FORMIS is hosted by CSE and is accessible from the CSE Home Page, it is NOT, in any way, an official CSE repository. It is being operated as a user web site with a "research" agenda. That agenda is stated above.

The current maintainer of the FORMIS archive is:

Milan Kuchta
Senior Scientific Advisor, INFOSEC
Communications Security Establishment.

mkuchta@manitou.cse.dnd.ca
VOICE: (613) 991-7353 (with voicemail)
FAX: (613) 991-7323

Common Criteria Draft Released on CD-ROM;

also available for downloading

A CD-ROM containing the initial release of the Common Criteria (Version 0.9, dated 31 October 1994), was distributed as planned at a panel session during the Tenth Annual Computer Security Applications Conference, in Orlando, Florida. It was to be distributed at similar sessions held in Europe within a few days. The document is approximately 800 pages printed.

Panelists at the Florida session were Steve La Fountain and Mario Tinto of NSA, Gene Troy of NIST, members of the editorial board that produced the document, and Lynne Ambuel, executive secretary. The countries cooperating on this document are the US (both NSA and NIST), Canada, United Kingdom, France, and Germany. It is intended to harmonize the existing evaluation criteria now in use in all of those countries and, eventually, to supersede them.

The document, as described during the panel session, embraces the notions of "protection profiles", developed in the draft US Federal Criteria released about two years ago, and "targets of evaluation" (TOE), from the European Information Technology Security Evaluation Criteria (ITSEC).

The panelists acknowledged that the released draft is inconsistent and incomplete, but solicited review and comment. They particularly invited discussion of whether the general scheme meets its stated goals, whether system developers/user/evaluators will be able to use it effectively, and whether there are significant omissions or inconsistencies.

See the "Interesting Links" section of this issue for URLs for downloading either full ascii, compressed ascii, or compressed PostScript of the document. See also Cynthia Irvine's Tenth ACSAC report for more information.

COAST to offer Gopher Service
by Gene Spafford

This note is actually two invitations related to the COAST security

archive. In early 1994, IBM provided a grant to COAST (Computer Operations, Audit, and Security Technology) to establish a net-accessible archive of security information. This project was then enhanced with the generous gift by Sun Microsystems of hardware for the archive server.

Several months ago, we went on-line with a comprehensive ftp archive (URL: <ftp://coast.cs.purdue.edu/pub>). The archive contains nearly 400 MB of tools, papers, technical reports, documentation, announcements, alerts, security patches, and newsletters. We continue to add to this archive on a daily basis. Before the end of December, the archive will also be available via a gopher server (URL: <gopher://coast.cs.purdue.edu>), with ``jughead" and ``Essence" indices. There is currently a link to the archive from the current COAST top-level WWW page (URL <http://www.cs.purdue.edu/coast/coast.html>).

We would like to invite you to browse the archive. Please feel free to copy whatever looks useful to you. All the material present is available via anonymous ftp and (soon) gopher. You may make copies subject to any copyright restrictions present in the individual files.

We also invite you to contribute to the archive. If you know of any on-line security-related materials available for public distribution that are not in the archive, please let us know. This includes material available via ftp, gopher, WWW, and WAIS. We will be happy to include the material in the archive, or as links in the server pages. In particular, we would like to mirror or copy any of your files, tools, theses, newsletters, and other security-related information so that others may find them when they browse our archive.

We have identified the following as areas of particular interest:

- access control
- artificial life
- authentication
- criminal investigation
- cryptography
- e-mail privacy enhancement
- firewalls
- formal methods
- general guidelines

- genetic algorithms
- incident response
- institutional policies
- intrusion detection
- law ethics
- malware (viruses, worms, etc.)
- network security
- password systems
- policies
- privacy
- risk assessment
- security related equipment
- security tools
- social impacts
- software forensics
- software maintenance
- standards
- technical tips
- the computer underground

If you know of material you think should be added, please send mail to security-archive@cs.purdue.edu and tell us what you have and where we can get a copy. In order of preference, we would prefer to get:

- a pointer to the source ftp/gopher/WWW site for a package
- a pointer to a mirror ftp/gopher/WWW site for the package
- a uuencoded tar file
- a shar file
- a CD-ROM
- a diskette or tape (QIC, 8mm, etc)

If you are providing software, we encourage you to ``sign" the software with PGP to produce a standalone signature file. This will help to ensure against trojaned versions of the software finding their way into the archive. We also suggest you think about getting Betsi signatures on your contributions (see </pub/doc/authentication/Betsi.ps.Z>) as an additional means of certifying your package.

If you have any comments or questions, please send e-mail to security-archive@cs.purdue.edu. Happy browsing!

Eugene H. Spafford
Director, COAST Project and Laboratory
Department of Computer Sciences
1398 Computer Science Building
Purdue University
West Lafayette, IN 47907-1398

spaf@cs.purdue.edu
<http://www.cs.purdue.edu/people/spaf>

Report on Tenth Annual Computer Security Applications Conference
December 5-9, 1994, Orlando, Florida
by Cynthia Irvine

The Tenth Annual Computer Security Applications Conference met in Orlando, Florida from December 5 to December 9, 1994. The conference was attended by approximately 275 individuals. In a change from previous conferences, the organizing committee chose not to supply attendees with conference-related paraphernalia and gave everyone a free pass into Disney World's Pleasure Island. This offered a wide variety of evening activity choices ranging from comedy to rock and dancing. The conference hotel was within walking distance of Disney World's Marketplace and Pleasure Island and we were fortunate to have pleasant weather, so there was ample opportunity for exploring that corner of the Disney empire.

COMMON CRITERIA

An important event on the afternoon prior to the official start of the conference was the U.S. debut of a preliminary draft of the Common Criteria for Information Technology Security Evaluation. [I was involved in a tutorial during the presentation, so this report is the result of subsequent interviews.] As presented, the Common Criteria are intended to provide a language for expressing commonality among existing criteria. A question from the audience was if incompatible criteria were described in a meta-framework, wouldn't they still be incompatible. There was no precise answer to this question. In off-line discussions, vendors voiced the need for involvement of those in the commercial world in formulating the criteria.

The criteria are approximately 800 pages long. Instead of bringing paper copies to the conference, the NSA folks brought 3.5 inch floppies and CDs. This was a great idea, since lugging two reams of paper home from the conference wasn't my idea of weight training fun. Those who would like to obtain a copy of the criteria and a copy of the reviewer's guide should contact NCSC at (410) 859 4458. NCSC has recently formed C7A, of which Keith Bruso is the chief, to handle the incorporation of comments into the Common Criteria. He informed me that NIST may be putting together a copy of the draft for ftp. Readers may wish to check at csrc.ncsl.nist.gov.

No additional public meetings regarding the draft Common Criteria are scheduled between now and the 1 March 1994 due date for comments. Those readers with accounts on Dockmaster can check accessible vendor and criteria fora for ongoing discussion of the criteria. Should future workshops be planned, formal invitations will be issued to those who provided comments. According to Bruso, such workshops will be organized as cooperative, international efforts and the logistics of any workshop could be complex. A May time frame is a likely possibility. The Canadian security conference and the IEEE symposium in Oakland could add to the scheduling challenges.

The goal for the Common Criteria's authors is to incorporate comments and fill in the remaining "TBD"s. The speed at which this takes place will depend upon the staffing that each of the international participants applies to the effort. A last draft, which will be available for review, will be the result of the current work. Bruso indicated that the earliest this draft will emerge is at the time of the NCSC Conference next fall, but that an early 1996 distribution was quite possible. This will be followed by another review period and subsequent consolidation.

FIRST PLENARY SESSION

The conference started on Wednesday, December 7 with introductions from Conference Chair Ann Marmor-Squires.

Keynote Address

The keynote speaker was Barbara Valeri, from OSD, who described an "era

of living dangerously" in which the current Department of Defense strategy for computer security was one of risk management rather than risk avoidance. Two examples were given:

First, Valeri noted that DoD has such a "strong addiction to technological enhancement" that new capabilities are run at risk rather than insuring their security. The Internet was cited as an example of a new capability that now cannot be turned off. It was noted that, despite statements to the contrary, Milnet and the Internet are not separated and that daily intrusions result. One Pentagon system suffered 4300 intrusion attempts over a 3 month period. Another system recorded evidence of hackers from fourteen different countries. A sample of Internet service providers indicated that 24 out of 29 were compromised. She described two choices for "Internet Death": fire (firewalls) and ice (isolation). She said that today we operate at risk of great loss with the threat of an Internet "Pearl Harbor Day."

Her second example was with respect to the dangers introduced by modern information retrieval tools which are likely to enhance the threat of security compromises by insiders. In the past, C3 information was controlled through pre-coordination and the need to know. Now information is provided for multiple purposes and is widely shared, e.g. for mission requirements, disaster relief, NATO allies, etc. Aggregation is seen as desirable by military commanders today. Unfortunately, the users of information are unknown and information retrieval tools make information more readily available to both the right people and the bad guys. She noted that there is a need for strong authentication and dynamic, flexible ways to establish commonalities of interest for information sharing. Again she noted the lack of total separation between classified and unclassified information and the growing push toward a multilevel operational environment.

She gave us her computer security wish list:

1. a cryptographic service providing management of cryptographic keys and certificates. The MISSI program was cited as an effort directed at addressing some of these issues.
2. controls on access to information, perhaps through something like an interoperable security grid on the Internet
3. audit, most likely through firewalls which, to quote Ben Franklin, allow you to "love your neighbor, but don't pull down the hedge."

Distinguished Lecture

For Don Parker, of SRI International, this is a special year. His topic was "Computer Loss Experience and Predictions." The text of his talk was available as a handout rather than as a part of the conference proceedings, which contains a one page synopsis entitled "Some Bumper Sticker Statements About Information Security." He started with the assertion that if business could have had a say in the matter, then the TCSEC would have been rejected. Who knows, but his talk was lively and full of information. For example, we learned that computer criminals are most successful when their thefts involve the correct amount of money: if too little or too much is taken one will be caught. Funds transfer thefts in the \$5M range are best, rather than at \$50 or \$50M.

Parker noted that although the frequency of business crime is decreasing, that of computer crime is increasing, so that eventually all business crime will be computer related. Nine types of computer crime were described:

1. computer larceny in the form of stealing of computer equipment. To counter this he suggested the use of serial number registration services for identification and recovery.
2. automated hacking. To counter this, he advocated automated rapid response techniques to detect and track intrusions.
3. desk-top forgery. Because the use of paper is not likely to be phased out entirely by electronic commerce in the foreseeable future, techniques to create unforgeable paper documents will be needed.
4. information anarchy. For this Parker advocates escrowed strong encryption, tempered by the use of electronic grand juries instead of a single judge to authorize government decryption of network transmissions. His statement that individuals should not be guaranteed the right to absolute privacy as a justification for escrowed encryption was not met with agreement from all sectors of the audience.
5. Extortion and sabotage using Trojan horse and logic bomb attacks. To counter this threat, the speaker advocated the use of audit and management techniques.
6. Internet abuse. This was described as the use of the Internet for purposes ranging from pedophilia to extreme advocacy groups. As in the case information anarchy, the speaker endorsed the use of strong escrowed encryption as a way to combat this problem. [Again, our desire

for an open society and law enforcement must be balanced.]

7. LAN-archy. This occurs when organizations use multiple LANs which are undocumented by the information security department. Such systems become vulnerable to unidentified information flow possibilities.

Better configuration management is required to solve this problem.

8. International industrial espionage. Parker suggested that treaties might provide limits to this kind of activity.

9. electronic data interchange fraud. The use of digital signatures, which may be accompanied by painful litigation to establish legal precedents, may offer a solution to this problem.

In summary, the speaker advocated many methods for combating computer crime, however, it was interesting to note that the use of trusted systems was not among the possible solutions presented.

At this point, Gary Smith, the Program Chairman sent us off to the sessions, which ran in concurrent tracks.

DISTRIBUTED SECURITY SESSION

"A Practical Approach to High Assurance Multilevel Computer Service" was presented by Judy Froscher and her colleagues at NRL. It constituted an extension to the body of SINTRA work that has already emerged from that group. First developed as a high assurance replica controller for backend database systems, this paper suggested that, as long as the backend systems were transaction-based, the SINTRA approach could be applied to a variety of legacy systems. A question from the audience regarding the number of access classes supported by a SINTRA system engendered a response that only a few classes would be supported such as TS, S, C, and U. Categories were relegated to "CMW enclaves," which is not a useful high assurance solution when label-based separation of categories is needed. [This was the first of several comments that this reviewer heard through the course of the conference in which categories were abandoned to enclave-like solutions.] In response to a question regarding SINTRA's performance, Froscher indicated that performance was good and that the network for their prototype was not swamped by replicas.

A paper entitled "Security Concerns for Distributed Systems" was presented by Mary Schanken, of NSA. The talk reviewed the notions presented in the December 1992 draft of the Federal Criteria [this

reporter has not had an opportunity to review the new Common Criteria in detail and is unable to comment regarding parallels with that document]. She noted the need for a new definition of assurance and for security policy parameters for cryptography, an important new functional component for secure distributed systems in this new view. The statement that functional components specified policy was made several times and appears in the text of paper as well. A question regarding the nature of channels elicited a response that channels are viewed as subjects. [Note that the historical introduction and bibliography did not cite the papers of Fellows et al.(1987) and Weissman (1992) describing distributed TCBs which dealt with INFOSEC.]

LouAnna Notargiacomo was the presenter of a multi-authored MITRE paper entitled "Security for the Common Object Broker Request Architecture (CORBA)." CORBA is a candidate object management standard for client/server computing which has received considerable attention from the commercial sector and international community. She noted that the security interfaces for CORBA were still very vaguely defined and that now was the time for members of the security community to become involved in the standard's definition. Desirable goals would be support of policy diversity through policy-independent solutions that did not prohibit extensions to the policy. This is a critical time to incorporate the requirements of multilevel security into the CORBA standards. More information can be obtained from the end user security group at the Object Management Group (OMG): request@omg.org and sec-wg@omg.org. Major commitment is required by vendors, since the entry fee is on the order of \$50,000.

ASSURANCE PANEL

My next stop was the panel discussion, "Reexamining Assurance," chaired by Marshall Abrams. . This panel was based on the results of two workshops. The first was a workshop held in March 1994 entitled "A Head Start on Assurance," the proceedings of which are available at [gopher://csrc.ncsl.nist.gov:71/00/nistir/assure.txt](http://csrc.ncsl.nist.gov:71/00/nistir/assure.txt) The second was a Workshop on Developmental Assurance that was held 16-17 June 1994. The premise of the panel was that current assurance methods are not meeting vendor or user needs and that new methods for establishing the assurance of products need to be pursued. The first speaker was Pat Toth from NIST. The second panelist was unable to attend.

Toth began by discussing the first workshop. The notion of a pedigree based on the identity and credentials of the creators of assurance evidence as a basis for the acceptability of assurance evidence was introduced. Thus if evidence was produced by a group with a good pedigree, perhaps less effort would need to be expended in examining the evaluation evidence. Considerable emphasis was placed on the value of metrics and testing and its importance in providing assurance. A conclusion of the workshop was that there should be a shift from "risk avoidance," which is considered to be too expensive, to "risk management."

The second workshop expanded upon the base of the first and emphasised the importance of relying upon the development process for assurance with the concomitant reduction of reliance on the evaluation.

A lively question and answer period followed: Are you formalizing incorrect advertising? The answer was that of course, one doesn't accept everything that a vendor says. Is assurance based on who does the evaluation rather than what they do? The response was that a "Consumer Reports" model would be good in which there were no criteria in advance and that products would be compared by testing. The panelists noted that there would have to be minimum standards. The panelist was asked whether a testing methodology, which could never be demonstrated to be complete, was preferable over a chain of evidence demonstrating that the security policy was enforced by the TCB. A member of the audience likened the problem of security with that of food and the FDA, stating that without regulations, labeling claims on food would state that "this stuff is great and tastes good" even when it was not very healthy for consumers. Some in the crowd asked whether one could really determine whether the existing criteria were subjective or objective.

A member of the audience pointed out that low assurance products were not created in a disciplined manner so that developmental assurance might not be applicable in such cases. She noted that instead one might want to establish requirements or standards for the time between the identification and repair of flaws.

When asked about distributed systems, Toth and Abrams noted that the process that they were considering did not work for networks and that knowing about security properties of individual products does not

necessarily translate into knowing something about the security properties of the system into which they are incorporated. Abrams suggested that instead of evaluating systems using composition, that decomposition techniques might be preferable.

A member of the audience asked how a consistent set of beliefs could be mapped to a consistent set of assurance criteria. The response from the panel indicated that there was no answer to that problem at this time.

SECOND PLENARY SESSION

After lunch, a plenary panel headed by Jody Heany, of MITRE, on "Secure Composition" was convened. Panelists were: Guy King, CSC; R. McAllister, NSA; R Oldach, DODISS Engineering Review Board; and Robert Wandell, NSA.

Heany began by describing five current government security initiatives:

- * Security Profiling
 - * DGSA (DoD Goal Security Architecture, which is available for ftp from NIST)
 - * DODIIS (DoD Intelligence Information System) and the DoD Technical Reference Model for Information Management definition of Core Products
 - * MISSI (Multilevel Information System Security Initiative)
 - * the NIST Application Portability Profile describing a profile of standards
- She asked whether these initiatives will solve composition issues and, from the user perspective, how consistent they were collectively.

Each speaker presented a brief description of the initiative with he was associated.

A question from the audience asked how various security policies were to interoperate. This was viewed as a a real problem, since one could not go to a catalog and compare policies. Another question related to reconciliation of the differences in security management of diverse systems. McAllister responded that one could not just compose a system and then "discover" a common policy, instead, policy must be known beforehand. It was also noted that some assistance was available using the DODIIS handbooks for system administrators.

DBMS SESSION

The next day I attended the database sessions. Myong Kang presented the first paper on the "Architectural Impact on Performance of a Multilevel Database System." The paper reported upon a series of simulation experiments to compare the performance of the SINTRA architecture with that of an ordinary single-level database used as a control. Variables included the time between the commit of one transaction and the start of another transaction; the type of transactions being performed; and the distribution of the user population across the security levels supported by SINTRA. The SINTRA model performed very well for retrieval dominated transactions, but for transactions dominated by update projections, lack of concurrency resulted in a performance degradation relative to the control.

The second paper, presented by Vinti Doshi, entitled "Benchmarking Multilevel Secure Database Systems," studied the performance differences between the TCB Subset and Trusted Subject trusted DBMS architectures. The researchers incorporated a label attribute for rows and attributes for polyinstantiation into the Wisconsin benchmark, which provided the raw data for the performance comparisons on join, select, sort, project, and aggregation experiments. Two COTS trusted DBMSs and two CMW platforms were examined and an untrusted DBMS was used as a control. The performance of the trusted subject DBMS versus the TCB subset DBMS was related to the operation tested.

The vendors attending the session were quite animated during the question and answer period that followed. Unfortunately, this effort was an internal project and the complete results are not available for public release. When asked about platforms, the author noted that comparisons of the two architectures were not conducted on the same underlying TCB base, which she noted was a worthwhile area for subsequent investigation. Caching became the focus of considerable discussion. Doshi noted that the effects of caching were eliminated by logging on and off between tests. It was noted by one vendor that most DBMSs cache across sessions and that logging on and off was inadequate and that the only way to eliminate the effects of caching would be to start each experiment from DBMS close. The author noted that the cache sizes of the underlying OSs were the same but concluded that further research was required to adequately consider the effects of caching.

The last paper, entitled "Organizing MLS Databases from a Data Modeling

Point of View," was presented by Gunter Pernul. The paper presented work on application-driven conceptual and logical design of a MLS relational database from an entity-relationship (ER) perspective. The use of semantic data modeling to achieve the conceptual design was discussed, but the majority of the presentation focussed on the logical design phase, particularly the problems associated with integrity constraints. Integrity constraints are a major headache in design of database applications. The authors noted that everything could actually be represented in first order logic, but that then the performance of the implementation suffered. Questions from the audience centered on the negative assignment log. Future work will explore trigger oriented and object oriented approaches.

AUDIT SESSION

[This report is via a conversation in the hall with an anonymous observer.]

The first paper, entitled "A Practical Approach to User Authentication," by M. Brown and S. Rogers, presented an extension of previous work on the use of keystroke analysis for authentication purposes. Three different techniques were used to analyze keystroking data obtained from an enlarged pool of impostors. It represents a continuation of established work in this area.

Paul Proctor presented the second paper on "Audit Reduction and Misuse Detection in Heterogeneous Environments: Framework and Application." A real-time audit reduction and analysis system, CMDS, has been developed which may be useful for those overwhelmed with audit data from heterogeneous systems. Our observer suggested that those interested in such tools should take a closer look.

The third paper, entitled "The Design of an Audit Trail Analysis Tool," by E. Fisch, G. White, and U. Pooch, addressed an interesting problem facing facilities in the aftermath of a serious intrusion: the sanitization of audit records. At many facilities, the staff may not be skilled enough to figure out what happened to them during an attack, so the best thing they can do is take their evidence to a CERT for analysis. A problem with this method is that the CERT may be able to determine details about an organization which one might not want to have revealed, e.g. proprietary information. In such cases, high level

sanitization of the audit records is needed before turning them over to the CERT. Four levels of sanitization were discussed and the method yielding the maximum information for the CERT is called "comprehensive sanitization." Tools to assist users in the sanitization process were described. Our observer found this paper to be rather interesting.

SECURE DBMS INTEROPERABILITY PANEL

Jack Wool moderated this session in place of the absent Joe Giordano. The objective of the presentations was to provide a status report on the PRISM (Portable, Reusable, Integrated Software Modules) program in multilevel database interoperability. The effort has examined near-term, practical solutions to productivity problems caused by airgaps between systems processing information at different security levels. The project builds upon the Air Force Electronics Systems Center effort to define solutions to non-MLS database interoperability problems by examining how COTS MLS databases in the TDI Class B1 assurance range might interoperate over a network. If solutions became available, problems in military mission planning, health care and financial systems could be addressed. The products examined were relational databases and legacy systems which ranged between Class B1 and Class B2, used some replication for survivability, and a variety of applications.

Some of the issues to be addressed are: gateway and middle ware capabilities, location transparency, multisite reads and joins, maximization of label sharing, and problems of DAC/MAC policy mismatches. Panelists were Rae Burns, AGCS; Don Brinkley, Sybase; Richard Allen, Oracle; Jess Worthington, Informix; and Doug Nelson, FSG.

Rae Burns gave a presentation on PRISM, the program, an effort to move existing and anticipated distributed system technology into the C4I context.

The scope of the effort has included: COTS products, read capability for data fusion, legacy sources, and trust for MLS interoperation. She noted that the effort is attempting to avoid vendor-dependent specialized products in favor of open and standard-based products.

She described a successful effort in trusted database interoperability

using the Sybase OmniSQL gateway, a SQL front end that is able to address queries to backends from Oracle, Sybase, and Informix. She observed that OmniSQL does not know about labels and that the labels from various vendors differ. The effort managed to perform a join between (1) Oracle7 and Trusted ORACLE7 and (2) Trusted Oracle7 and Secure SQL Server. The draft interoperability report is publicly available. Future efforts will include the NRaD look at a Remote Data Access (RDA) prototype.

Don Brinkley presented a number of features of the Sybase products, noting that Sybase does not duplicate operating system and network functions, e.g. label services. Architectural issues that must be addressed by vendors are threefold: first, the implementation of databases on heterogeneous operating systems; second, the interoperability of heterogeneous databases; and finally the, interoperability of heterogeneous trusted databases. He noted that Sybase has already addressed the first problem and that the architecture permits a Secure SQL Server to perform remote procedure calls to an Omni SQL Gateway to retrieve data from heterogeneous backend systems, thus yielding at least one potential solution to the other two problems.

Richard Allen focussed on labels. He started by observing that today only 15% of all stored information is in relational databases; the remainder is stored in hierarchical or flat databases. The amount of data stored in MLS databases is extremely small. Some problems that need to be addressed include standardization of SQL for MLS databases so that interoperation between vendors of MLS systems is possible. In addition, the syntax between trusted and untrusted databases should be the same. He mentioned that SecureWare's MaxSix protocols for security attribute passing can be used to interconnect legacy systems. A label cognizant version of Oracle's procedural language for SQL (PL/SQL) called PLEX (for PL/SQL Extensions) will enhance the development of MLS applications. Looking to the future, he observed that a prebuilt COTS gateway for MLS databases could be constructed, but that vendors will be wary of such an effort since it is not clear who would purchase it and the product might have a rather limited lifetime. If it were a one-time development then it is likely to be unsupported and for mission critical systems, this would be a problem.

Jess Worthington discussed incompatibilities between security policies.

He noted that the "ideal" would be a "global security policy." Unfortunately, today there is no language or semantics for discussing security policies. In the DBMS context, base models for BLP and Clark Wilson are needed. Polyinstantiation, downgrading, write up/down, etc. all need to be described. Each database needs a "profile" of its security policy so that databases can "connect" together sensibly. To achieve such interconnection, systems may have to negotiate common ground. He suggested that a middle-ware product, e.g. Remote Data Access (RDA), Distributed Computing Environment (DCE), etc., might be suitable and noted that a consortium is working on Secure RDA which will include encryption protocols for moving data across a network. He reminded us that these efforts include nothing to deal with labels. As a final question to the audience he asked: Can security policy be tailored on the fly?

Doug Nelson spoke about current needs for element level classification for labeling in multilevel databases in the context of command and control such as that associated with Scott AFB. Of the 4M lines of code in Ada and C++ for that effort, about 10,000 lines are trusted. He noted the need for trusted labels at the screen level provided through a trusted path, i.e. the user must be able to trust the label on the screen and, as systems evolve, that trust should be available with increased levels of assurance. With an enormous investment in existing code, portability to higher levels of assurance was desirable. He identified a number of issues that need to be addressed:

1. trusted data distribution
2. the messiness of polyinstantiation for applications. (He noted that at the table level polyinstantiation was controllable, but at higher granularity it became increasingly difficult to contend with.)
3. downgrading and the need for time-dependent downgrading.
4. models for the notion of privilege
5. problems associated with audit, and
6. MLS versions of ordinary RDBMS capabilities.

One practical solution might be an API layer able to interface with trusted products.

A member of the audience noted the problems associated with translating DBMS and application policies in addition to policy translation problems noted earlier. There was a question regarding the cascading problem [see the TNI] in combining various systems. The answer was that it was necessary to do something practical and to accept the risks of

cascading. Another question regarded the support for CMW policies. Informix noted that a stored procedure would permit users to augment the TCB.

Jack Wool may be contacted at woolj@tango-vs1.hanscom.af.mil or ESC/ENS, Bldg. 1704, Rm 203, Hanscom AFB, MA 01731-5000 or (617) 377 9374.

FIREWALLS SESSION

The first paper, "A Secure E-mail Gateway," was presented by R. Smith described a security architecture to permit E-mail connectivity between a large CMW-based (Class B1) DoD MLS network and a large, Class C2, unclassified network. In his introduction, the author described the perils of using a Class B1 system instead of a Class B2 through Class A1 system for interconnections. The solution was to use the Boeing Class A1 MLS LAN as the platform for an E-mail gateway. This system has a secure protocol stack. It was possible to eliminate interactive services such as TELNET and FTP so that only SMTP ports were available. The MLS LAN had to be modified to support the E-mail gateway and, as completed, provides a static environment since it is not reprogrammable. It supports the CIPSO extension to IP. The system is not perfect since it is still vulnerable to unauthorized disclosure on the part of insiders, but it provides a high level of assurance against externally mounted attacks.

One member of the audience asked about the maintenance of the ACLs for the DAC mechanism used to restrict the users of the gateway in a system with 60,000 users. Randell responded they restricted user access to the e-mail facility so that the ACLs wouldn't run out of space.

"The MITRE Security Perimeter," the second talk of the session, was presented by David Goldberg. The speaker described some of the MITRE management's motivation for establishing a strong security perimeter around the organization's systems. Most notable were the use of MITRE by the "wily hacker" and the unfavorable publicity MITRE received as a result of the "Internet worm." With systems located at many sites across the country, requirements for dial-in access by staff members, and the need to bar intruders, the establishment and maintenance of the security perimeter through the use of COTS products and customized techniques has been non-trivial. He described the implementation of the

security perimeter as phased effort and stated that they were now in Phase IV. Objectives of the effort were to: 1. reduce potential for data-driven attacks 2. use the Internet as a back bone to connect remote sites 3. improve security on external LANs. 4. use COTS products for secure identification This paper gives a valuable worked example of a security perimeter.

The last paper of the session was "EINet: A Secure, Open Network for Electronic Commerce" presented by D. Rosenthal of MCC EINet. As the paper in the proceedings does, the talk gave a description of the EINet product, a set of application-level tools designed to provide Internet security services. Rosenthal noted at the outset that, despite the location of the paper within the Firewalls session, EINet was not a firewall. The author described security requirements addressed by the product: 1. prevent unauthorized access to private on-line services, 2. protect confidential information, and 3. access to services. He noted that the product was intended to be portable and easy to use and includes components for: authentication, access control, communication, tool kits for user registration, and operational procedures. Authentication is Kerberos-based with enhancements for network time services and GUIs for users and integrators. It was noted that since this is an application-based system, it is vulnerable. A member of the audience asked whether the system incorporated duress alarms to which the response was no.

WANDERING AMONG SESSIONS

During the next interval, I went from session to session attempting to take in the papers that seemed most intriguing. First I attended a panel session entitled "Availability Theory and Fundamentals for Practical Evaluation and Use" moderated by K. Keus and M. Ullmann. Several points of view were represented. The moderators felt that it is possible to characterize system availability and operability in the same terms as used to describe confidentiality in the ITSEC and that criteria could be developed to permit the evaluation of availability. See their paper in the proceedings for details. Although I did not stay for the remainder of the session, two other perspectives were to be presented. First, fault tolerance as embodied in the systems of Tandem Computers was presented as a means of providing for availability by Wing Chan. Finally, Christoph Cordes was to state a position, which in his abstract starts with the statement that "'Availability' is not a

clearly defined term."

Then I went to the Security Engineering session picking up the end of Deborah Bodeau's talk on a "System-of-Systems Security Engineering." She was describing security engineering techniques that may be applied when viewing a collection of systems as an individual system, for example when connecting legacy systems. The paper gives guidance for inspecting the individual systems and considering their collective interaction. She noted that for risk analysis, with a structured approach complemented by an ad hoc approach, it may be possible to learn things about additional vulnerabilities. Typical problems encountered are incompatibilities between target architectures, territorialities of administrators, scalability, and information gathering. A member of the audience asked whether the described techniques resulted in an accreditation, to which the reply was that it hadn't because no one wanted to expend the effort to achieve one. She noted that a system of systems may require multiple policy models.

Next Mary Bernstein presented "AOS: An Avonics Operating System for Multilevel Secure Real-Time Environments," which describes an operating system which enforces hard real-time scheduling constraints and multilevel security in an embedded system. The real time kernel was written in Ada and included: secure initialization, access control and resource management, process management, event synchronization and time management, exception and error handling, I/O support, and an Ada RTS interface. A "System Build" concept based on a priori knowledge of all subjects and objects in the system and the use of premediation of accesses was key to achieving combined access control and real-time goals. Secure initialization is also done a priori using a "Postlinker." This "hardwiring" had a price though: a set of trusted tools becomes part of the TCB.

She concluded her talk by stating that this system demonstrated that one can have security in real time systems meeting Class B2-B3 criteria. [Close reading of the paper will permit readers to assess this statement for themselves.] When asked, she noted that the AOS system does not fit into the TCSEC since the radar process does not have login and authentication. When queried about covert channels she said that there was no requirement to close covert channels, but if they were closed, a performance degradation would be likely. She noted that the rendezvous of Ada was not used.

CMW SESSION

This set of presentations was moderated by Steve LaFountain.

The first paper was entitled "Ops/Intel Interface Lessons Learned: The Integrator's Perspective." It reported on the experiences of a team charged with integrating Ops/Intel workstations (OIW) into a real system so that, at workstations, analysts will be able to review and downgrade Sensitive Compartmented Information to Secret. The integrators faced many difficult choices while bringing together a system to execute both COTS and GOTS products on the CMW-based OIWs. Considerable retrofitting was required to make things work. Perhaps most interesting was their discussion of the filtering routers and the potential for new firewall technology to provide alternative solutions.

Clare Robinson presented a paper called "Using Security Models to Investigate CMW Design and Implementation." The motivation for this work was the possibility that at some sites the information labels of CMWs will be used in ways that had not been originally intended in CMW design. For example, in order to avoid the process of manual review and downgrading, some organizations would like to use information labels to label output rather than sensitivity labels, thus achieving automated downgrades. Their study resulted in models which may be used to analyze the approaches to information labels taken by vendors of various COTS CMW products. A major conclusion of this work was the need for "limited trust" in application software if information labels are used to determine the labeling output rather than sensitivity labels. It will be up to each organizations will have to assess the risks of using CMWs in unintended ways.

The final paper of this session gave us a big change of pace as R. Newman-Wolfe (a.k.a. Nemo) presented "Performance Analysis of a Method for High Level Prevention of Traffic Analysis using Measurements from a Campus Network," which isn't CMW research. In this paper he discussed the application of previous work to prevent traffic analysis by modifying network traffic to achieve spatial neutrality, i.e. uniform communications levels between nodes, in a network. The researchers observed traffic patterns on the University of Florida network and compared the cost of obtaining neutrality using two strategies: first,

padding traffic with additional packets and, second, applying rerouting to smooth traffic patterns followed by padding. The latter technique was less costly. In addition, they compared heuristic and linear programming techniques. He concluded his talk by discussing problems that might occur during a crisis when the volume of traffic changes drastically and noted that current solutions were not particularly attractive. When queried regarding the potential covert channel capacity from traffic analysis, he said that it could range between 100 to thousands of bits per second.

EDITORIAL PANELS

A final panel session of the conference was the Editorial Session, chaired by Ravi Sandu. The first editorialist was Bill Neugent, of MITRE, entitled "Where We Stand in MLS: Requirements, Approaches, Issues, and Lessons Learned." He said that the actual security needs in workstation environments are broader than current systems can provide. For example, multilevel security may be needed within a level, say SECRET, to separate war gaming, exercises, and mission information.

In current practice, the use of special category (SPECAT) is a problem for workstations. SPECAT control officers use common sense when dealing with data. Some sites have half of their data with SPECAT code words on it. A solution has been the use of stand alone PCs, which is not a particularly attractive choice. Meaningful use of MLS for SPECAT systems is needed.

Allied interoperation presents another set of problems for multilevel secure systems. Bilateral agreements can cause problems because classifications on information are not uniform. Where the U.S. will label something as CONFIDENTIAL, the ally may have a corresponding label "REALLY HOT STUFF", which makes the information sound more important than it really is. Today considerable human activity is required when determining the releasability of data.

He also noted that there is a problem with remote organizations which may have information which is topic-area specific and thus hard to automate. A result may be a "System High Culture." In some cases, system high was used on all sites so that one doesn't know what is or is not secret. Another problem area is that of unpredictable

aggregation. An example was given of a system in which case-by-case labeling had to be applied to the reports from the DBMS. This is laborious and error-prone.

He summarized with several lessons learned:

1. Users need buy into the benefits of MLS.
2. When integrating MLS into systems, use testing and think about the people using the system.
3. Labels can become too complex. Three or four simple labels were suggested as an alternative to the confusion that can result from the use of very complicated labels.
4. Better configuration management is needed. If given a choice, then the people in the field will only do some high level specifications and some penetration testing, whereas configuration management of all levels is needed.
5. System management should be improved so that cumbersome, error-prone tasks can be streamlined.

His bottom line was that we should proceed with caution and that to address many of these issues additional research will be needed.

In the discussion that followed, it was noted that there are no rules of thumb regarding distinctions between sensitive and proprietary information. Some countries require that all MLS systems be certified. A member of the audience noted that categories are important. Unfortunately, the policies regarding categories are not always well stated. Another comment from the audience noted that there are problems at home as well, for example some people at certain U.S. government agencies (State) appear to think that C2 is penetration resistant. A final comment noted that, in the future, data-driven attacks through firewalls are likely to become a serious problem.

[At this point I had to catch a plane.]

This was a conference with something for everyone as far as content and continued a tradition of fostering interaction between a variety of security communities. The conference committee should be commended for an excellent job.

Report on 31st Internet Engineering Task Force Meeting

by Avi Rubin

The Internet Engineering Task Force (IETF) held its 31st meeting in San Jose, CA on Dec. 3-9, 1994. The IETF has a mosaic home page, <http://www.ietf.cnri.reston.va.us/home.html>, where more information can be found. Briefly, the IETF is the protocol engineering and development arm of the Internet. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, network management, security, etc.).

The December meeting had an estimated 1200 participants. Every morning began with a technical presentation of interest to everyone. For example, Nat Borenstein gave a presentation on First Virtual Holdings, a company that performs electronic commerce on the Internet. Then, the groups broke up into their areas of interest.

The interest in the security working groups and BOF's was apparent from the number of people standing in the back during the sessions because all the seats were full. There were various working groups including IPSEC (IP layer security), CAT (Common authentication Technologies), DNS security, PEM security, Authenticated Firewall Traversal (AFT), and two BOF (bird of feather) sessions on object security and world wide web security.

The IPSEC working group met three times. The first meeting consisted of a lively, unproductive debate about byte alignments for the IP layer headers. The group seemed unable to decide what had been agreed upon at the previous meeting, and did not accomplish much. The key management meeting was much more useful. Several key management schemes were presented with varying features and requirements. It was determined that several of the schemes can be merged, while others are needed as well because they handle different requirements, such as multicast. Someone presented a table of the proposed systems and their respective requirements. The next step is to assign weights. The biggest open question that is under debate on the mailing list right now is whether or not perfect forward secrecy is needed. That is, is the computational

cost of preventing the compromise of a master key from compromising all session keys worth it?

The PEM meeting was very short. The group voted to adopt the new version of PEM created by TIS. The two BOF sessions, object security and WWW security resulted in decisions to form working groups. The groups are now trying to create their charters to seek approval. The PEM meeting was very short. The group voted to adopt the new version of PEM created by TIS.

The next IETF meeting will be in Danvers, Massachusetts on April 3-7, 1995.

Calls for Papers

(see also Calendar)

- o Conferences

- o New Security Paradigms Workshop '95, La Jolla, California, 22-25 August 1995. This workshop seeks radical new models for computer security, trusted system integration, and intercomputer networking security. The goal is to develop transcendent solutions that provide the flexibility and interoperability users require in trusted systems. To participate, submit, preferably via email, a research paper or a 5-10 page position paper to Program Chairs John Dobson (John.Dobson@newcastle.ac.uk) and Catherine Meadows (meadows@itd.nrl.navy.mil) by email by April 1, 1995. Alternatively, submit five copies of a hard-copy paper to either program chair by March 24, 1995.
 - o Communications and Multimedia Security (IT - Sicherheit[Security] '95), Graz, Austria, 20-21 September, 1995. Joint working conference of IFIP TC-6, IFIP TC-11, and Austrian Computer Society. Topics of interest primarily in the area of professional communication and multimedia application in relation to security aspects, including High speed communications security, Encryption for communication, Communications security aspects in multimedia, Escrow technologies, Certification mechanisms, Decentralized trust and certification, Electronic money for charging multimedia services, Legal aspects of communications security, and Social and ethical aspects of communications security. Papers (in

English) due 28 Feb. 1995 via e-mail (LaTeX or RTF or postscript format) to Prof. Reinhard Posch, e-mail: rposch@iaik.tu-graz.ac.at
Proceedings planned to be published as IFIP document by Chapman and Hall.

- o Fourth International Conference on Computer Communications and Networks, 20-23 Sept. 1995, Las Vega, Nevada. Topics of interest listed are primarily oriented towards networking; includes network security. Manuscripts, including abstract, limited to 5000 words; six copies due by March 17, 1995 to program chair, Prof. Kia Makki (kia@unlv.edu), c/o Ms. Chris Nienaber, National Supercomputing Center for Energy and the Environment, 4505 Maryland Parkway, Box 454028, Las Vega, Nevada, 89154-4028. Tel (702)895-4024, fax (702)895-4156 Conference information available from ic3n@cacs.usl.edu Workshop and tutorial proposals also solicited; contact Prof. Niki Pissinou, U of SW Lousiana, (pissinou@cacs.usl.edu, Tel(318)482-6604, fax (318)482-5791
- o First International Workshop on Multi-Media Database Management Systems, 28-30 August 1995, Blue Mountain Lake, NY. Areas of interest listed center on multi-media databases, including access security issues. Four copies of paper not exceeding 25 double-spaced pages, including abstract, figures, pictures, etc.[no multi-media submissions?--ed.] due by 15 February 95 to Dr. Kingsley Nwosu, AT&T Bell Labs, 67 Whippany Rd., Rm 2C-256, Whippany, NJ 07981-4211, e-mail: nwosuck@harpo.wh.att.com, phone (201)386-4211, fax(201)386-2182

Reader's Guide to Current Technical Literature in Security and Privacy

Part 1: Conference Papers

Papers to be presented at the Internet Society Symposium on Network and Distributed SYstems Security, San Diego, CA, February 16-17, 1995, as listed in the preliminary program distributed December 7, 1994.

Multicast-Specific Security Threats and Counter-Measures, Tony Ballardie and Jon Crowcroft (University College London, United Kingdom).

Design of a Key Agile Cryptographic System for OC-12c Rate ATM, Daniel Stevenson, Nathan Hillery, Greg Byrd, and Dan Winkelstein

(Microelectronics Center of North Carolina - MCNC, USA).

IpAccess: An Internet Service Access System for Firewall Installations, Steffen Stempel (University of Karlsruhe, Germany).

Security for the Internet Protocol (IP) and IP Next Generation, Paul A. Lambert (Motorola, USA).

Security for the Internet Domain Name System, James M. Galvin (Trusted Information Systems, USA).

Security of Routing Protocols in the Internet, Gary Scott Malkin (Xylogics, USA).

Security Approaches to Routing in the Internet, Sandra L. Murphy (Trusted Information Systems, USA).

Trusted Distribution of Software Over the Internet, Aviel D. Rubin (Bellcore, USA). Location-Independent Information Object Security, John Lowry (Bolt Beranek and Newman, USA).

Electronic Cash on the Internet, Stefan Brands (Centrum voor Wiskunde en informatica - CWI, The Netherlands).

NERD: Network Event Recording Device: An Automated System for Network Anomaly Detection and Notification, David G. Simmons and Ronald Wilkins (Los Alamos National Laboratory, USA).

An Overview of SNIF: A Tool for Surveying Network Information Flow, Jim Alves-Foss (University of Idaho, USA).

Distributed Audit Trail Analysis, Abdelaziz Mounji, Baudouin Le Charlier, Denis Zampunieris and Naji Habra (Facultes Universitaires de Namur - FUNDP, Belgium).

SESAME V2 Public Key and Authorisation Extensions to Kerberos, Piers McMahon (ICL, United Kingdom).

Yaksha: Augmenting Kerberos with Public Key Cryptography, Ravi Ganesan (Bell Atlantic, USA).

GSS-API Security for ONC RPC, Barry Jaspan (OpenVision Technologies, USA).

A Certificate Management System: Structure, Functions and Protocols, Nada Kapidzic and Alan Davidson (Stockholm University & Royal Institute of Technology, Sweden).

PEMToolKit: Building a Top-Down Certification Hierarchy for PEM from the Bottom Up, Alireza Bahreman (Bellcore, USA).

A New Approach to the X.509 Framework: Allowing a Global Authentication Infrastructure

Without a Global Trust Model, Suzan Mendes (TS-E3X - Research and Development Center, France) and Christian Huitema (INRIA, France).

Reader's Guide to Current Technical Literature in Security and Privacy
Part 2: Journal and Newsletter Articles, Book Chapters

- o Pernul, G. Database security. in Advances in Computers, Vol. 38, Academic Press, 1994, ISBN 0-12-012138-7, pp.1-72.
- o ACM Computing Surveys, Vol. 26, No. 3 (Sept. 1994), Carl E. Landwehr, Alan R. Bull, John P. McDermott, William S. Choi. A taxonomy of computer program security flaws. pp.211-254.
- o Scientific American, Vol. 271, No. 5 (Nov. 1994), Jeffrey I. Schiller. Secure distributed computing. pp. 54-58.
- o Computers & Security Volume 13</i>, Number 6. (Elsevier) Refereed Papers:
Michel Denault, Dimitris Gritzalis, Dimitris Karagiannis and Paul Spirakis. Intrusion detection: approach and performance issues of the SECURENET system. pp. 495-507.
- Bhavani Thuraisingham. Security issues for federated database systems. pp. 509-526.
- Peter Ladkin and Harold Thimbleby. Comments on a paper by Voas, Payne and Cohen: 'A model for detecting the existence of software corruption in real time'. pp. 527-531.

Reader's Guide to Current Technical Literature in Security and Privacy
Part 3: Books

Denning, D. and H. Lin, eds. Rights and Responsibilities of Participants in Networked Communities. Computer Science and Telecommunications Board, National Research Council, National Academy Press, Washington, DC, Dec., 1994, ISBN 0-309-0590-1, 160pp.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. Thunder's Mouth Press, NY, ISBN 1-56025-080-1, 432pp., \$22.95.

Calendar

Dates	Event, Location	Point of Contact/ more information
-------	-----------------	------------------------------------

-----	-----	-----
-------	-------	-------

Calendar

Updated 12 January 1995

Date (Month/Day/Year), Event, Locations, e-mail for more info, Hyperlink
(if any)

1/14/95: COMPASS '95 papers due; rushby@csl.sri.com or
 ftp.csl.sri.com

2/ 3/95: CSFW-8 papers due; gong@csl.sri.com

2/13/94: papers due, 5th USENIX Sec Symp, Utah; securityauthors@usenix.org

2/15/95- 2/16/95: FISSEA Conference; grice@micf.nist.gov(Tammy Grice)

2/16/95- 2/17/95: ISOC-Symp, San Diego; gcarrier@mitre.org
 (Gloria Carrier)

2/28/95: IT-Sicherheit '95 papers due; rposch@iaik.tu-graz.ac.at

3/ 1/95: NCSC-18 papers due; NCS_Conference@Dockmaster.ncsc.mil

3/10/95: SAC '95 ext. abstracts due; sac95@scs.carleton.ca

3/17/95: DCCA-5 papers due; morganti@settimo.italtel.it

3/20/95: IFIP WG11.3 papers due; ting@eng2.uconn.edu (T.C.Ting)

3/24/95: NSPW '95 papers due (hardcopy); meadows@itd.nrl.navy.mil

3/31/95: MDS-95, papers due, York, England; IMACRH@V-E.ANGLIA.AC.UK

4/ 1/95: NSPW '95 papers due (e-mail); { John.Dobson@newcastle.ac.uk AND

meadows@itd.nrl.navy.mil}

4/ 3/95: IEEE S&P 5-min talk abstracts due; meadows@itd.nrl.navy.mil
5/ 1/95- 5/ 6/95: 6th Nat'l OPSEC Conf, Albuquerque; (301)982-0720 (voice)
5/ 7/95- 5/12/95: IEEE S&P 95; dmj@mitre.org (registration)
5/ 9/95- 5/11/95: IFIP/SEC '95 Capetown; IFIPSEC95@RKW.RAU.AC.ZA
5/16/95- 5/19/95: 7th CCSS, Ottawa; CCSS7@cse.dnd.ca
5/18/95- 5/19/95: SAC '95, Ottawa; sac95@scs.carleton.ca
5/22/95- 5/24/95: Eurocrypt '95, France; iacr95@ccett.fr
6/ 5/95- 6/ 7/95: 5th USENIX Sec Symp, Utah; conference@usenix.org
(registration)
6/13/95- 6/15/95: CSFW-8, Ireland; s.foley@cs.ucc.ie
6/26/95- 6/30/95: COMPASS '95; BONNIE.DANNER@trw.sprint.com
8/13/95- 8/16/95: IFIP WG11.3, New York (RPI); ting@eng2.uconn.edu (T.C.Ting)
8/27/95- 8/31/95: Crypto'95 Santa Barbara; tavares@ee.queensu.ca
8/22/95- 8/25/95: NSPW '95 San Diego (UCSD); meadows@itd.nrl.navy.mil
9/ 5/95- 9/ 6/95: MDS-95, York, England; IMACRH@V-E.ANGLIA.AC.UK
9/20/95- 9/21/95: IT-Sicherheit '95; rposch@iaik.tu-graz.ac.at
9/27/95- 9/29/95: DCCA-5, Champaign, IL; no e-mail address available
10/10/95-10/13/95: NCSC-18, Baltimore; NCS_Conference@Dockmaster.ncsc.mil
3/??/96: CCS-3, New Delhi; exact dates to be available 1/95
5/ 5/96- 5/ 8/96: IEEE S&P 96; no e-mail address available
5/ 5/96- 6/ 9/96: IFIP/SEC 96-Greece; no e-mail address available
11/??/96: ESORICS '96, Rome, Italy; no e-mail address available
5/ 4/97- 5/ 7/97: IEEE S&P 97; no e-mail address available

Key:

CCS-2 = 2nd Annual ACM Conference on Computer and Communications Security
CCSS = 7th Annual Canadian Computer Security Symposium
CSFW = Computer Security Foundations Workshop
DCCA = Dependable Computing for Critical Applications
ESORICS = European Symposium on Research in Computer Security
FISSEA = Federal Information Systems Security Educators' Association
IEEE S&P = IEEE Symposium on Research in Security and Privacy
IFIP/SEC = International Conference on Information Security (IFIP TC11)
IFIP WG11.3 = IFIP WG11.3 9th Working Conf. on Database Security
MDS '95 = Second Conf. on the Mathematics of Dependable Systems
NCSC = National Computer Security Conference
NSPW = New Security Paradigms Workshop
ISOC-Symp = Internet Society 1995 Symposium on Network and
Distributed System Security
SAC '95 = 2nd Annual Workshop on Selected Areas of Cryptography

USENIX Sec Symp = USENIX UNIX Security Symposium

Who's Where: recent address changes

Submitted 3 January 1994:

Jeff DeMello
Security Evaluations Manager
Oracle Corporation
500 Oracle Parkway, Box 659405
Redwood Shores, CA 94065

415-506-8797 phone
415-506-7221 fax
jdemello@us.oracle.com

Submitted 20 December 1994:

Cristi Garvey
Sybase, Inc.
Atrium SE 320
1650 65th Street
Emeryville, CA 94608

510-922-4802
cristi@sybase.com

Interesting Links

Format:
Description (first line) followed by URL (second line)

Government sources/information:

Library of Congress source for on-line legislation
<http://thomas.loc.gov>

Common Criteria links:
directory of full ascii files:

<http://www.itd.nrl.navy.mil/ITD/5540/cc>
directory of compressed (ZIP'ed) PostScript and ascii files:
<http://csrc.ncsl.nist.gov/nistpubs/>

Web Server for the US Office of the Secretary of Defense:
<http://enterprise.osd.mil/>

Federally-Funded Research in the U.S. (not a US Govt. server)
<http://medoc.gdb.org/best/fed-fund.html>

Professional societies and organizations:

IFIP TC11 - Security & Protection in Information Processing (Experimental)
http://www.iaik.tu-graz.ac.at/tc11_hom.html

IFIP TC6 (Communication Systems)
http://www.iaik.tu-graz.ac.at/tc6_home.html

Other places for interesting research papers and announcements

Framework and Open Reference Model for Information Security (FORMIS)
<http://moowis.cse.dnd.ca/~formis>

Purdue COAST home page
<http://www.cs.purdue.edu/coast>

CMU NetBill Project home page; electronic commerce information
<http://www.ini.cmu.edu/netbill/>

Trusted Information Systems home page
<http://www.tis.com/>

Graz University of Technology,
Institute for Applied Information Processing and Communications
<http://www.iaik.tu-graz.ac.at/iaik.html>

TC Publications for Sale

We have a few surplus copies of the proceedings of the Oakland conference
(199N IEEE Symposium on Research in Security and Privacy) available for

purchase by TC members at favorable rates. Current issues in stock and prices are as follows:

Price by mail			
from TC IEEE CS Press IEEE CS Press			
Year	TC members	IEEE member price	List Price
----	-----	-----	-----
1992	\$15	\$43	\$86
1993	\$20	\$30	\$60
1994	\$30	\$30+\$4 S&H	\$60+\$5 S&H

For overseas delivery:

-- by surface mail, please add \$5 per order (3 volumes or fewer)

-- by air mail, please add \$10 per volume

to the prices listed above.

If you would like to place an order, please send a letter specifying

o which issues you would like,

o where to send them, and

o a check in US dollars, payable to the 1995 IEEE Symposium on Security and Privacy to:

Charles N. Payne

Treasurer, IEEE TC on Security and Privacy

Code 5542

Naval Research Laboratory

Washington, DC 20375-5337

U S A

Sorry, we are not yet ready for electronic commerce!

TC Officer Roster

Chair:

Terry Vickers Benz

Trusted Information Systems

11340 W. Olympic Blvd, Suite 265

Los Angeles, CA 90064

(310) 477 - 5828

tcvb@la.tis.com

Vice Chair:

Deborah Cooper

Director, Information Systems Security

Unisys Govt. Information Systems Group

12010 Sunrise Valley Drive

Reston, VA 22091

(703)847-3895

cooper@rtc.reston.paramax.com

Newsletter Editor:	Standards Subcommittee Chair
Carl Landwehr	[VOLUNTEER NEEDED!]
Code 5542	
Naval Research Laboratory	
Washington, DC 20375-5337	
(202)767-3381	
Landwehr@itd.nrl.navy.mil	

Information for Subscribers and Contributors

SUBSCRIPTIONS: To subscribe, send e-mail to <cipher-request@itd.nrl.navy.mil> (which is NOT automated) with subject line "subscribe". To remove yourself from the subscription list, send e-mail to cipher-request@itd.nrl.navy.mil with subject line "unsubscribe".

Those with access to hypertext browsers may prefer to read Cipher that way.

It can be found at URL

<http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher>

CONTRIBUTIONS: to <cipher@itd.nrl.navy.mil> are invited. Cipher is a NEWSletter, not a bulletin board or forum. It has a fixed set of departments, defined by the Table of Contents. Please indicate in the subject line for which department your contribution is intended. For Calendar entries, please include an e-mail address for the point-of-contact. **ALL CONTRIBUTIONS CONSIDERED AS PERSONAL COMMENTS; USUAL DISCLAIMERS APPLY.** All reuses of Cipher material should respect stated copyright notices, and should cite the sources explicitly; as a courtesy, publications using Cipher material should obtain permission from the contributors.

ARCHIVES: Available at URL

<http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/cipher-archive.html>

=====end of Electronic Cipher Issue #3, 1/13/95=====